ABELIAN COVERINGS OF FINITE GENERAL LINEAR GROUPS AND AN APPLICATION TO THEIR NON-COMMUTING GRAPHS

AZIZOLLAH AZAD, MOHAMMAD A. IRANMANESH, CHERYL E. PRAEGER, AND PABLO SPIGA

Abstract. In this paper we introduce and study a family $\mathcal{A}_n(q)$ of abelian subgroups of $\mathrm{GL}_n(q)$ covering every element of $\mathrm{GL}_n(q)$. We show that $\mathcal{A}_n(q)$ contains all the centralisers of cyclic matrices and equality holds if $q > n$. Also, for $q > 2$, we prove a simple closed formula for the size of $\mathcal{A}_n(q)$ and give an upper bound if $q = 2$.

A subset X of a finite group G is said to be pairwise non-commuting if $xy \neq yx$, for distinct elements x, y in X. As an application of our results on $\mathcal{A}_n(q)$, we prove lower and upper bounds for the maximum size of a pairwise non-commuting subset of $\mathrm{GL}_n(q)$. (This is the clique number of the non-commuting graph.) Moreover, in the case where $q > n$, we give an explicit formula for the maximum size of a pairwise non-commuting set.

For the 100th anniversary of the birth of B. H. Neumann

1. Introduction

In a finite general linear group $\mathrm{GL}_n(q)$ the class of *cyclic matrices* (see Section 1.1 for the definition) plays an important role both algorithmically (see [16]), and in representation theory (for the recognition of irreducible representations). This paper uncovers a new role in which cyclic matrices help to determine the maximum size $\omega(\mathrm{GL}_n(q))$ of a set of *pairwise non-commuting* elements of $\mathrm{GL}_n(q)$, or equivalently the clique number of the non-commuting graph for this group. The study of these clique numbers for various families of groups goes back to the 1976 paper

2000 *Mathematics Subject Classification.* 20B25.

Key words and phrases. General linear group, cyclic matrix, non-commuting subsets of finite groups, non-commuting graph.

Address correspondence to A. Azad, Department of Mathematics, Arak University, Arak 38156-879, Iran; E-mail: a-azad@araku.ac.ir

The paper forms part of the Australian Research Council Federation Fellowship Project FF0776186 of the third author. The fourth author is supported by UWA as part of the Federation Fellowship project. The second author is supported by Research Council of Yazd University.

[14] of B. H. Neumann, answering a question of Paul Erdös, and inspired much subsequent research. A short account is given in Subsection 1.1 to contextualise our results. Our paper is written in honour of the 100th anniversary of B. H. Neumann's birth on 15 October 1909. Our results on $\omega(\mathrm{GL}_n(q))$ can be summarised as follows in terms of the quantity

$$l(q) = \prod_{k=1}^{\infty} (1-q^{-k})^{-k(k+1)/2-1}. \tag{1.1}$$

Theorem 1.2. *For $q \geq 2$,*

$$q^{-n}(1-q^{-3}-q^{-5}+q^{-6}+q^{-n}) \leq \frac{\omega(\mathrm{GL}_n(q))}{|\mathrm{GL}_n(q)|} \leq q^{-n} l(q)$$

and moreover

$$l(q) \leq \begin{cases} 1+2q^{-1}+7q^{-2}+114q^{-3} & \text{if } q \geq 3 \\ 395.0005 & \text{if } q = 2. \end{cases}$$

We comment separately below on our strategies for proving the lower bound and the upper bound. These involve on the one hand existing estimates for the proportion of cyclic matrices in $\mathrm{GL}_n(q)$ (for the lower bound), and on the other hand a new investigation of a family $\mathcal{A}_n(q)$ of abelian subgroups of $\mathrm{GL}_n(q)$ covering every group element.

1.1. **Cyclic matrices and the lower bound.** An element $g \in \mathrm{GL}_n(q)$ is cyclic if its characteristic polynomial is equal to its minimal polynomial.

Definition 1.3. We denote by $\mathcal{N}_n(q)$ the set of *centralisers of cyclic matrices* in $\mathrm{GL}_n(q)$, that is, $\mathcal{N}_n(q) = \{C_{\mathrm{GL}_n(q)}(g) \mid g \text{ cyclic in } \mathrm{GL}_n(q)\}$. Also, we denote by $N_n(q)$ the cardinality $|\mathcal{N}_n(q)|$.

The centralisers of cyclic matrices in $\mathrm{GL}_n(q)$ are abelian and small (when compared with centralisers of non-cyclic matrices). Moreover they cover a *large* fraction of the elements of $\mathrm{GL}_n(q)$. It turns out that results of Neumann and Praeger [15], and more precise results obtained independently by Fulman [9] and Wall [21], can be applied almost directly to give a very good lower bound on $N_n(q)$ and on $\omega(\mathrm{GL}_n(q))$.

Theorem 1.4.

$$\frac{\omega(\mathrm{GL}_n(q))}{|\mathrm{GL}_n(q)|} \geq \frac{N_n(q)}{|\mathrm{GL}_n(q)|} \geq q^{-n}(1-q^{-3}-q^{-5}+q^{-6}-q^{n}).$$

1.2. **An abelian covering and the upper bound.** Centralisers of cyclic matrices do not cover every element in $\mathrm{GL}_n(q)$ (see Remark 3.3 at the end of Section 3). Therefore, in Definition 1.6 below we define a family $\mathcal{A}_n(q)$ of abelian subgroups of $\mathrm{GL}_n(q)$, which contains $\mathcal{N}_n(q)$ and covers every element of $\mathrm{GL}_n(q)$, giving an upper bound for $\omega(\mathrm{GL}_n(q))$. We prove moreover that $\mathcal{N}_n(q) = \mathcal{A}_n(q)$ when $q > n$.

Theorem 1.5. (a)**:** $\mathrm{GL}_n(q) = \cup_{A\in\mathcal{A}_n(q)} A$.

(b)**:** $\omega(\mathrm{GL}_n(q)) \leq |\mathcal{A}_n(q)|$ *with equality if and only if* $q > n$.

(c)**:** $\mathcal{N}_n(q) \subseteq \mathcal{A}_n(q)$ *with equality if and only if* $q > n$.

Thus we need to determine $|\mathcal{A}_n(q)|$. It seems, on consulting several of our colleagues that the family $\mathcal{A}_n(q)$ has not been studied previously. This surprised us, considering the central role it plays in Theorem 1.5. The set $\mathcal{A}_n(q)$ is defined as follows.

Definition 1.6. Let V be the n-dimensional vector space k^n over the field k of size q. Let $\mathcal{A}_n(q)$ be the set of abelian subgroups A of $\mathrm{GL}_n(q)$ such that the A-module V has a decomposition $V_1 \oplus \cdots \oplus V_r$ into indecomposable A-modules satisfying the following properties:

(i)**:** $A = A_1 \times \cdots \times A_r$, where $A_i \subseteq \mathrm{GL}(V_i)$;

(ii)**:** for $i = 1, \ldots, r$, we have $A_i = C_{\mathrm{GL}(V_i)}(a_i)$, for some element $a_i \in \mathrm{GL}(V_i)$ such that V_i is an indecomposable $\langle a_i\rangle$-module.

It is shown in Proposition 5.9 that, for $q > 2$, the elements in $\mathcal{A}_n(q)$ are maximal abelian subgroups of $\mathrm{GL}_n(q)$. The bulk of the paper is devoted to determining the limiting size of $\mathcal{A}_n(q)$ for a fixed field size $q > 2$ and large n.

Theorem 1.7. *For $q > 2$, the sequence $\{q^n|\mathcal{A}_n(q)|/|\mathrm{GL}_n(q)|\}_{n\geq 0}$ is increasing with limit $l(q)$, as defined in Equation 1.1, and we have*

$$\left| q^n \frac{|\mathcal{A}_n(q)|}{|\mathrm{GL}_n(q)|} - l(q) \right| = o(r^{-n/2})$$

for every positive $r < q$. For $q = 2$, there exists an increasing sequence $\{2^n b_n\}_{n\geq 0}$ with limit $l(2)$ such that $|\mathcal{A}_n(2)|/|\mathrm{GL}_n(2)| \leq b_n$, and we have

$$|2^n b_n - l(2)| = o(r^{-n/2})$$

for every positive $r < 2$.

The sequence $\{b_n\}_{n\geq 1}$ can be found in Definition 6.1. Our method is to study the generating function $F(t) = \sum_n^\infty a_n t^n$, where $a_n = |\mathcal{A}_n(q)|/|\mathrm{GL}_n(q)|$ and $a_0 = 1$ (see Definition 6.1). For $q > 2$ we obtain a simple formula for $F(t)$. In fact, using the theory of symmetric functions we prove the following result.

Theorem 1.8. *If $q > 2$, then*

$$F(t) = \left(\prod_{i=0}^{\infty}(1 - q^{-(i+1)}t)^{-1}\right)\left(\prod_{m\geq 2, i,j\geq 0}(1 - q^{-(i+j+2m-1)}t^m)^{-1}\right).$$

Moreover, $F(t)$ has a simple pole at $t = q$ and $(1 - q^{-1}t)F(t)$ is analytic on a disk of radius $q^{3/2}$.

It would be interesting to know if a similar formula could be obtained for $F(t)$ when $q = 2$.

Remark 1.9. *The coefficient of degree n in $F(t)$ equals $|\mathcal{A}_n(q)|/|\mathrm{GL}_n(q)|$ which also equals $\omega(\mathrm{GL}_n(q))/|\mathrm{GL}_n(q)|$ when $q > n$, by Theorem 1.5 (b). In particular, the equation for $F(t)$ in Theorem 1.8 can be used to obtain explicit formulas for $\omega(\mathrm{GL}_n(q))$ when $q > n$.*

We present in Table 1 $|\mathcal{A}_n(q)|$, for $1 \leq n \leq 6$ and $q > 2$.

n	$\lvert\mathcal{A}_n(q)\rvert$
1	1
2	$q^2 + q + 1$
3	$q^6 + q^5 + 3q^4 + 3q^3 + q^2 - q - 1$
4	$q^{12} + q^{11} + 4q^{10} + 7q^9 + 9q^8 + 5q^7 + 2q^6 - 3q^5 - 2q^4 - q^3 + q^2 + q$
5	$q^{20} + q^{19} + 4q^{18} + 9q^{17} + 18q^{16} + 22q^{15} + 22q^{14} + 15q^{13} + 6q^{12} - 4q^{11} - 7q^{10}$ $-6q^9 - 2q^8 + q^7 + 2q^6 + q^5 - q^4 - q^3$
6	$q^{30} + q^{29} + 4q^{28} + 10q^{27} + 23q^{26} + 40q^{25} + 60q^{24} + 65q^{23} + 68q^{22} + 53q^{21}$ $+33q^{20} + 5q^{19} - 8q^{18} - 19q^{17} - 16q^{16} - 7q^{15} + q^{14} + 6q^{13} + 6q^{12} + 5q^{11}$ $-q^9 - q^8 + q^7 + q^6$

TABLE 1.

In the next subsection, we recall how the problem of determining the maximum size $\omega(G)$ of a pairwise non-commuting set of elements arises in group theory. Also, we recall some results on $\omega(G)$, for various families of groups, and we see how our method generalises some results in the literature [1, 2].

1.3. **The non-commuting graph of a group.** In 1976, B. H. Neumann [14] answered a question of Paul Erdős about the maximal *clique* size in the *non-commuting graph* $\Gamma(G)$ of a group G, namely the graph with vertices the elements of G and with edges the pairs $\{x, y\}$ with $xy \neq yx$. A clique in a graph is a set of pairwise adjacent vertices and hence in $\Gamma(G)$ a clique is a *pairwise non-commuting subset of* G. In group theoretic language, Erdős asked whether there exists a finite upper bound on the cardinalities of pairwise non-commuting subsets of G, assuming that every such subset is finite. Neumann proved that the family of groups satisfying the condition of Erdős is precisely the class of groups G in which the centre $Z(G)$ has finite index, and he proved moreover that for such groups G, each pairwise non-commuting subset of G has size at most $|G : Z(G)| - 1$. Neumann's answer inspired much subsequent research, for example [1, 2, 3, 4, 6, 13, 17, 19].

We let $\omega(G)$ denote the *maximum cardinality* of a pairwise non-commuting subset of G. Because of Neumann's result, the study of groups G such that $\omega(G) < \infty$ is reduced to the study of finite groups. It follows from results of [17] that, if $n = |G : Z(G)|$, then $c \log_2 n \leq \omega(G) \leq n - 1$, for some positive constant c. The lower bound is achieved with $c = 1$ by each extraspecial 2-group. (According to [3, 17], this was proved by Isaacs.)

On the other hand the upper bound is achieved for the quaternion group $G = Q_8$ and the dihedral group $G = D_8$ of order 8, both of which have $\omega(G) = 3$. It is believed that groups G which are "close" to being nonabelian simple will have $\omega(G)$ "close" to the upper bound. Indeed, for the symmetric group $\mathrm{Sym}(n)$ of degree n $\omega(\mathrm{Sym}(n))$ satisfies the bounds in Table 2, where a, b, c, d are constants, see [4, Theorem 1].

Lower bound	comments
$a(n-2)!$	for every n
$d(\log\log n)(n-2)!$	for infinitely many n
Upper bound	
$b(\log\log n)(n-2)!$	for every n
$c(n-2)!$	for infinitely many n

TABLE 2. Results for $\omega(\mathrm{Sym}(n))$ from Brown [4]

Also, for finite general linear groups $\mathrm{GL}_n(q)$, if $q > 2$ then $\omega(\mathrm{GL}_2(q)) = q^2 + q + 1$ (see [1, Lemma 4.4]), and if $q > 3$ then $\omega(\mathrm{GL}_3(q)) = q^6 + q^5 + 3q^4 + 3q^3 + q^2 - q - 1$

(see [2, Theorem 1.1]). These two results on the finite general linear group prove the bounds of Theorem 1.2 for $n \leq 3$ and the values for $\omega(\mathrm{GL}_n(q))$ (for $n = 2, 3$) are exactly the second and third row in Table 1.

Finally, it was conjectured [2, Conjecture 1.2] that, for $q > n$, the number $\omega(\mathrm{GL}_n(q))$ should be somewhat larger than $q^{n^2-n} + q^{n^2-n-1} + (n-1)q^{n^2-n-2}$. As we discuss in Remark 7.10, this conjecture is incorrect for $n \geq 6$.

Using the results of [10] a lower bound for $\omega(G)$ similar to that provided by Theorem 1.2 can be obtained for all finite classical groups G. It would be interesting to know if a similar estimation for a class of abelian subgroups of classical groups could be carried out to yield a good upper bound for $\omega(G)$ for these groups.

1.4. **Structure of the paper.** In this final introductory section we briefly summarise where the proofs of the theorems stated in Section 1 are given.

Proof of Theorem 1.2. The lower bound is a direct application of Theorem 1.4. From Theorem 1.5 we have $\omega(\mathrm{GL}_n(q)) \leq |\mathcal{A}_n(q)|$ and from Theorem 1.7 the sequence $\{q^n|\mathcal{A}_n|/|\mathrm{GL}_n(q)|\}_n$ is increasing with limit $l(q)$. Therefore the upper bound follows. The estimates on $l(q)$ are collected in Lemma 7.1 in Section 7. $\square$

Proof of Theorem 1.4. The proof of this result is given in Section 2. $\square$

Proof of Theorem 1.5. This theorem is proved in Section 5. Namely, Part (a) is proved in Proposition 5.1, Part (b) (which is an application of Part (a)) is proved in Corollary 5.13 and Part (c) is proved in Theorem 5.11. $\square$

Proof of Theorem 1.7. This result in proved in Sections 6 and 7. Namely, in Theorem 6.16 we prove that the sequences $\{q^n|\mathcal{A}_n(q)|/|\mathrm{GL}_n(q)|\}_n$ (for $q > 2$) and $\{q^n b_n\}_n$ (for $q = 2$) are increasing. In Theorem 7.8 we compute the rate of convergence and the limit. $\square$

Proof of Theorem 1.8. The equation for the generating function $F(t)$ is proved in Theorem 6.15. The rest of the theorem follows from Propositions 7.3 and 7.6. $\square$

2. Lower bound: Proof of Theorem 1.4

Recall that an element g in $\mathrm{GL}_n(q)$ is said to be a *cyclic matrix* if the characteristic polynomial of g is equal to its minimum polynomial, see [15]. If g is a cyclic matrix, then (see [15, Theorem 2.1(3)]) the group $C_{\mathrm{GL}_n(q)}(g)$ is abelian and by [15, Corollary 2.3] we have $|C_{\mathrm{GL}_n(q)}(g)| \leq q^n$. Thus the groups in $\mathcal{N}_n(q)$ (see Definition 1.3) are abelian of order at most q^n.

Cyclic matrices of $\mathrm{GL}_n(q)$ are well-studied (see [10, 15]) and in particular Wall (see [10, page 2]) proved that the proportion $c_{\mathrm{GL}}(n,q)$ of cyclic matrices in $\mathrm{GL}_n(q)$ satisfies

$$\left| c_{\mathrm{GL}}(n,q) - \frac{1-q^{-5}}{1+q^{-3}} \right| \leq \frac{1}{q^n(q-1)}.$$

Thus

$$c_{\mathrm{GL}}(n,q) \geq \frac{1-q^{-5}}{1+q^{-3}} - \frac{1}{q^n(q-1)} > 1-q^{-3}-q^{-5}+q^{-6}-q^{-n}, \tag{2.1}$$

where the second inequality is obtained by expanding $(1-q^{-5})/(1+q^{-3})$ in powers of q and by noticing that $1/q^n(q-1) \leq 1/q^n$. Using this remarkable result, we easily obtain Theorem 1.4.

Proof of Theorem 1.4. Let $\mathcal{C}_n(q)$ denote the set of cyclic matrices of $\mathrm{GL}_n(q)$ and $X = \{(g,C) \mid g \in \mathcal{C}_n(q), C \in \mathcal{N}_n(q), g \in C\}$. We claim that every element g of $\mathcal{C}_n(q)$ lies in a unique element of $\mathcal{N}_n(q)$. Indeed, assume $g \in C_1, C_2$, for some $C_1, C_2 \in \mathcal{N}_n(q)$, and let g_1, g_2 be cyclic matrices such that $C_i = C_{\mathrm{GL}_n(q)}(g_i)$, for $i = 1,2$. As C_1, C_2 are abelian and $g \in C_1, C_2$, we get $C_1, C_2 \subseteq C_{\mathrm{GL}_n(q)}(g)$. Similarly, as $C_{\mathrm{GL}_n(q)}(g)$ is abelian and $g_i \in C_i \subseteq C_{\mathrm{GL}_n(q)}(g)$, we get $C_{\mathrm{GL}_n(q)}(g) \subseteq C_i$ and $C_{\mathrm{GL}_n(q)}(g) = C_1 = C_2$.

Counting the size of the set X, we have

$$\begin{aligned} q^n N_n(q) &= q^n|\mathcal{N}_n(q)| = \sum_{C\in\mathcal{N}_n(q)} q^n \geq \sum_{C\in\mathcal{N}_n(q)} |C \cap \mathcal{C}_n(q)| = |X| \\ &= \sum_{g\in\mathcal{C}_n(q)} |\{C \in \mathcal{N}_n(q) \mid g \in C\}| = \sum_{g\in\mathcal{C}_n(q)} 1 = |\mathcal{C}_n(q)| = |\mathrm{GL}_n(q)| c_{\mathrm{GL}}(n,q). \end{aligned}$$

Now Equation 2.1 yields $N_n(q) \geq q^{-n}|\mathrm{GL}_n(q)|(1-q^{-3}-q^{-5}+q^{-6}-q^{-n})$.

It remains to prove that $\omega(\mathrm{GL}_n(q)) \geq N_n(q)$. Let $C_1, \ldots, C_r$ be the distinct elements of $\mathcal{N}_n(q)$, with $r = N_n(q)$. Let g_i be a cyclic matrix in $\mathrm{GL}_n(q)$ such that $C_i = C_{\mathrm{GL}_n(q)}(g_i)$, for $i = 1, \ldots, r$. Set $S = \{g_i \mid 1 \leq i \leq r\}$. We claim that, if

$i \neq j$, then the group elements g_i and g_j of S do not commute. If $g_ig_j = g_jg_i$, then $g_j \in C_{\mathrm{GL}_n(q)}(g_i) = C_i$, whereas we showed above that C_j is the unique element of $\mathcal{N}_n(q)$ containing g_j. This yields $\omega(\mathrm{GL}_n(q)) \geq |S| = r = N_n(q)$ and thus the theorem follows. □

3. Upper bound: idea of the proof

In the rest of this paper, we determine an upper bound for $\omega(\mathrm{GL}_n(q))$ (and hence for $N_n(q)$ by Theorem 1.4). Also, for $q > n$, we prove that $N_n(q) = \omega(\mathrm{GL}_n(q))$ and we obtain an exact formula for $N_n(q)$. Before going into more detail, in this section we briefly describe the method that is used. First, our results rely on this elementary observation.

Lemma 3.1. *Let G be a group and $\mathcal{A}$ be a collection of abelian subgroups of G such that $G = \cup_{A \in \mathcal{A}} A$. We have $\omega(G) \leq |\mathcal{A}|$.*

Proof. Let S be a pairwise non-commuting set. Since $A \in \mathcal{A}$ is abelian, we get $|S \cap A| \leq 1$. As $G = \cup_{A \in \mathcal{A}} A$, we obtain $|S| \leq |\mathcal{A}|$. Thus the result follows. □

Lemma 3.1 can be used effectively to obtain upper bounds for $\omega(G)$. As an example we derive Brown's upper bound for $\omega(\mathrm{Sym}(n))$ mentioned in Subsetion 1.3, see [4, Theorem 1 (1)].

Proposition 3.2. *There exists a constant b, which does not depend on n, such that $\omega(\mathrm{Sym}(n)) \leq b(\log \log n)(n-2)!$.*

Proof. By [8, Theorem 2], the number of maximal abelian subgroups of $\mathrm{Sym}(n)$ is at most $b(\log \log n)(n-2)!$, for some constant b not depending on n. Thus the proposition follows from Lemma 3.1. □

Unfortunately, there is no natural description (as in $\mathrm{Sym}(n)$) for the maximal abelian subgroups of $\mathrm{GL}_n(q)$. So, it looks particularly difficult to give an upper bound for the number of all maximal abelian subgroups of $\mathrm{GL}_n(q)$. (For some results on the number of maximal abelian subgroups with trivial unipotent radical in Chevalley groups, we refer the reader to [20].) We overcome this difficulty by focusing only on the subfamily $\mathcal{A}_n(q)$ of abelian subgroups defined in Definition 1.6 which is large enough to cover all the group elements as will be proved in Proposition 5.1. This leads to an upper bound for $\omega(\mathrm{GL}_n(q))$. For $q > n$, we construct

a pairwise non-commuting set of size $|\mathcal{A}_n(q)|$ and so we obtain an explicit formula for $\omega(\mathrm{GL}_n(q))$.

Remark 3.3. We note that, for general q and n, centralisers of cyclic matrices do not cover all the elements in $\mathrm{GL}_n(q)$. Here we simply give an example for $\mathrm{GL}_4(2)$. Consider the matrix

$$x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

With an easy computation, it is easy to check that

$$C = C_{\mathrm{GL}_4(2)}(x) = \left\{ \begin{pmatrix} 1 & 0 & 0 & a \\ b & 1 & c & d \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_2 \right\}$$

and that C has order 16. In particular, C consists of unipotent elements. A unipotent matrix u is cyclic if and only if u has minimum polynomial $(t-1)^4$, that is, $u-1$ has rank 3. Now, it is easy to see that if $c \in C$, then $c-1$ has rank at most 2. Therefore, C contains no cyclic matrix and hence x is not contained in the centraliser of a cyclic matrix.

A similar example can be constructed for every $q > 2$. Namely, consider the matrix

$$x = \begin{pmatrix} D & 0 \\ 0 & U \end{pmatrix}$$

in $\mathrm{GL}_{2q-1}(q)$, where D is a $(q-1)\times(q-1)$-diagonal matrix with distinct eigenvalues and U is a $(q\times q)$-cyclic matrix with minimum polynomial $(t-1)^q$ (that is, a regular unipotent element of $\mathrm{GL}_q(q)$). It is possible to show that x is not contained in the centralizer of a cyclic matrix of $\mathrm{GL}_{2q-1}(q)$.

4. Conjugacy classes and centralisers in $\mathrm{GL}_n(q)$

In this section, we introduce some notation and some well-known results that are going to be used throughout the rest of the paper.

Let k be a field with q elements, V be k^n and $k[t]$ be the polynomial ring with coefficients in k. Now, each element g of $\mathrm{GL}_n(q)$ acts on the vector space V and hence defines on V a $k[t]$-module structure by setting $tv = gv$. We denote this $k[t]$-module by V_g. For instance, it is easy to see that g is a cyclic matrix if and only

V_g is a cyclic $k[t]$-module. Clearly, any two elements g, h of $\mathrm{GL}_n(q)$ are conjugate if and only if V_g and V_h are isomorphic $k[t]$-modules.

For each element g of $\mathrm{GL}_n(q)$, there exist unique $s, u \in \mathrm{GL}_n(q)$ such that $g = su = us$, where s is *semisimple* and u is *unipotent* (see [5, Section 1.4]). We call s (respectively u) the semisimple (respectively unipotent) part of g.

A unipotent element u of $\mathrm{GL}_n(q)$ is said to be a *regular unipotent* element if $u - 1$ has rank $n - 1$, that is u has minimum polynomial $(t - 1)^n$ and so u is a cyclic matrix. In particular, regular unipotent elements of $\mathrm{GL}_n(q)$ form a $\mathrm{GL}_n(q)$-conjugacy class. In the following lemma, we collect some well-known information on the centraliser and normaliser of a regular unipotent element.

Lemma 4.1. *Let u be a regular unipotent element of $\mathrm{GL}_n(q)$, for $n \geq 2$. The group $C = C_{\mathrm{GL}_n(q)}(u)$ is abelian of order $(1 - q^{-1})q^n$ and $N_{\mathrm{GL}_n(q)}(C)$ has order $(1 - q^{-1})^2 q^{2n-1}$.*

Proof. Set $v = u - 1$. Since u is a regular unipotent element, the element v is a nilpotent matrix of rank $n - 1$ with minimal polynomial t^n. Also, $C_{\mathrm{GL}_n(q)}(u) = C_{\mathrm{GL}_n(q)}(v)$. The elements centralizing v are the isomorphisms of the $k[t]$-module V_v. Since $V_v \cong k[t]/(t^n)$ is a uniserial module, it is readily seen (see for example [15, page 265]) that $\mathrm{End}_{k[t]}(V_v)$ is a polynomial ring in v isomorphic to $k[t]/(t^n)$. Therefore, $\mathrm{End}_{k[t]}(V_v) = \langle 1, v, \ldots, v^{n-1} \rangle$ is abelian. Since the ideals of $k[t]/(t^n)$ are in one-to-one correspondence with the ideals of $k[t]$ that contain (t^n) and (t) is the unique maximal ideal containing (t^n), it follows that $\mathrm{End}_{k[t]}(V_v)$ is a local ring with maximal ideal $(v) = \langle v, \ldots, v^{n-1} \rangle$ and every element of (v) is nilpotent. In particular, the element $x = \sum_{i=0}^{n-1} a_i v^i$ of $\mathrm{End}_{k[t]}(V_v)$ is invertible if and only if $x \notin (v)$, that is $a_0 \neq 0$. This shows that C is abelian of order $q^n - q^{n-1} = (1 - q^{-1})q^n$.

Let $x = \sum_{i=0}^{n-1} a_i v^i$ be in $\mathrm{End}_{k[t]}(V_v)$. We claim that x is a regular unipotent element if and only if $a_0 = 1$ and $a_1 \neq 0$. Assume first that x is a regular unipotent element. Thus $x - 1$ is a nilpotent element with minimum polynomial t^n. Now, $x - 1$ is nilpotent if and only if $a_0 - 1 = 0$, that is $a_0 = 1$. Also, as $(v^2)^m = 0$ for every $m \geq n/2$, we obtain that $x - 1$ is not a multiple of v^2, that is $a_1 \neq 0$. Conversely, assume that $a_0 = 1$ and $a_1 \neq 0$. In particular, $x - 1 = vy$, where by the previous paragraph y is an invertible element of $\mathrm{End}_{k[t]}(V_v)$. So, $(x - 1)^{n-1} = v^{n-1}y^{n-1} \neq 0$ and $x - 1$ has minimum polynomial v^{n-1}. Thus x is a regular unipotent element. This yields that C contains $q^{n-1} - q^{n-2} = (1 - q^{-1})q^{n-1}$ regular unipotent elements.

Since the regular unipotent elements form a $\mathrm{GL}_n(q)$-conjugacy class, C contains $(1-q^{-1})q^{n-1}$ regular unipotent elements and $C = C_{\mathrm{GL}_n(q)}(u')$ for each regular unipotent element $u' \in C$, we have that $|N_{\mathrm{GL}_n(q)}(C)|/|C| = (1-q^{-1})q^{n-1}$ and $|N_{\mathrm{GL}_n(q)}(C)| = (1-q^{-1})^2 q^{2n-1}$. □

Let $d, m \geq 1$ be integers such that $n = dm$ and E be a field extension over k of degree d. As E is a k-vector space of dimension d and d divides n, we have that k^n is isomorphic to E^m as k-vector spaces. Under this isomorphism, the group $\mathrm{GL}_m(q^d)$ embeds into a subgroup of $\mathrm{GL}_n(q)$, which we still denote by $\mathrm{GL}_m(q^d)$. This does not cause any confusion because all fields of order q^d are isomorphic, and therefore different embeddings give rise to subgroups which are conjugate.

We recall that, given a group G, a G-module V is said to be *indecomposable* if $V \neq 0$ and if it is impossible to express V as a direct sum of two non-trivial G-submodules. In the next lemma we determine the elements g of $\mathrm{GL}_n(q)$ such that V_g is indecomposable.

Lemma 4.2. *Let g be in $\mathrm{GL}_n(q)$ such that V_g is an indecomposable $k[t]$-module, where g has semisimple part s and unipotent part u. Then g is a cyclic matrix with minimum polynomial f^m, for some irreducible polynomial f of degree d with $dm = n$. Replacing g by a conjugate if necessary, $g \in \mathrm{GL}_m(q^d)$, the element s is a scalar matrix of $\mathrm{GL}_m(q^d)$ corresponding to a generator of $\mathbb{F}_{q^d}$ and the element u is a regular unipotent element of $\mathrm{GL}_m(q^d)$. In particular, $C_{\mathrm{GL}_n(q)}(g)$ is abelian of order $(1-q^{-d})q^{dm}$.*

Proof. Since $k[t]$ is a principal ideal domain, we have that the $k[t]$-module V_g is a direct sum of cyclic modules of the form $k[t]/(f^m)$, where f is a monic irreducible polynomial of $k[t]$ and $m \geq 1$. As V_g is indecomposable, we obtain that $V_g \cong k[t]/(f^m)$, for some irreducible polynomial $f = t^d - \sum_{i=1}^{d} a_i t^{i-1}$ of degree d and $n = dm$. Let $J(f)$ denote the companion matrix for the polynomial f

$$J(f) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & & & & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_1 & a_2 & & \cdots & a_d \end{pmatrix}$$

and let

$$J_m(f) = \begin{pmatrix} J(f) & I_d & 0 & \cdots & 0 \\ 0 & J(f) & I_d & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \\ \vdots & & \ddots & J(f) & I_d \\ 0 & \cdots & \cdots & 0 & J(f) \end{pmatrix}$$

with m diagonal blocks $J(f)$. By construction the characteristic polynomial of the block matrix $J_m(f)$ equals f^m. Also, [12, Example 1, page 140] shows that f^m is the minimum polynomial of $J_m(f)$. Therefore $J_m(f)$ is a cyclic matrix. As V_g and $V_{J_m(f)}$ are $k[t]$-modules isomorphic to $k[t]/(f^m)$, we obtain that g is conjugate to $J_m(f)$ and so g is a cyclic matrix with minimum polynomial f^m. Thus we may assume that $g = J_m(f)$. So, s is obtained from $J_m(f)$ by replacing the $d \times d$-identity matrix I_d with the $d \times d$-zero matrix 0. Similarly, u is obtained from $J_m(f)$ by replacying the $d \times d$-matrix $J(f)$ with the $d \times d$-identity matrix I_d.

Now, the centraliser of the cyclic matrix $J(f)$ in the algebra of $d \times d$-matrices over k is a polynomial algebra isomorphic to $k[t]/(f)$. Since f is irreducible, $k[t]/(f)$ is a field of size q^d. Hence $C_{\mathrm{GL}_d(q)}(J(q))$ is a cyclic group of order $q^d - 1$ isomorphic to the multiplicative group of a field of size q^d and, since f is irreducible, $J(f)$ corresponds to a generator in this field. Under this identification, $J_m(f)$ is an element of $\mathrm{GL}_m(q^d)$, s is a scalar matrix correspoding to a generator of $\mathbb{F}_{q^d}$ and u is a regular unipotent matrix. The rest of the lemma follows from Lemma 4.1. $\square$

Corollary 4.3. *Let g_1 and g_2 be in $\mathrm{GL}_n(q)$ such that V_{g_1} and V_{g_2} are indecomposable $k[t]$-modules. Set $C_{g_i} = C_{\mathrm{GL}_n(q)}(g_i)$, for $i = 1, 2$. The following are equivalent:*

- (i)**:** *C_{g_1} is conjugate to C_{g_2};*
- (ii)**:** *g_1 and g_2 have minimum polynomials $f_{g_1}^m$ and $f_{g_2}^m$, for some irreducible polynomials f_{g_1}, f_{g_2} of degree d with $dm = n$;*
- (iii)**:** *the C_{g_1}-module V is isomorphic to the C_{g_2}-module V.*

Proof. By Lemma 4.2, g_i is a cyclic matrix with minimum polynomial $f_{g_i}^{m_{g_i}}$, for some irreducible polynomial f_{g_i} of degree d_{g_i} with $d_{g_i} m_{g_i} = n$ (for $i = 1, 2$). Assume C_{g_1} is conjugate to C_{g_2}. By Lemma 4.2, $|C_{g_1}| = (1 - q^{-d_{g_1}})q^{d_{g_1} m_{g_1}}$ and $|C_{g_2}| = (1 - q^{-d_{g_2}})q^{d_{g_2} m_{g_2}}$. As $|C_{g_1}| = |C_{g_2}|$, we have $d_{g_1} = d_{g_2}$ and $m_{g_1} = m_{g_2}$. Thus Part (i) implies Part (ii).

Assume Part (ii). Let s_1 and s_2 be the semisimple parts of g_1 and g_2, respectively. Similarly, let u_1 and u_2 be the unipotent parts of g_1 and g_2, respectively. By Lemma 4.2, replacing g_1 and g_2 by a conjugate if necessary, we may assume that $g_1, g_2 \in \mathrm{GL}_m(q^d)$, s_1 and s_2 are scalar matrices corresponding to generators of $\mathbb{F}_{q^d}$ and u_1, u_2 are regular unipotent elements of $\mathrm{GL}_m(q^d)$. Therefore $C_{g_i} = C_{\mathrm{GL}_n(q)}(g_i) = C_{\mathrm{GL}_m(q^d)}(g_i) = C_{\mathrm{GL}_m(q^d)}(u_i)$, for $i = 1, 2$. Since regular unipotent elements form a $\mathrm{GL}_m(q^d)$-conjugacy class, we obtain that u_1 is conjugate to u_2 in $\mathrm{GL}_m(q^d)$ and so $C_{g_1} = C_{\mathrm{GL}_m(q^d)}(u_1)$ is conjugate to $C_{g_2} = C_{\mathrm{GL}_m(q^d)}(u_2)$ and Part (i) follows.

If C_{g_1} is conjugate in $\mathrm{GL}_n(q)$ to C_{g_2}, then the C_{g_1}-module V is isomorphic to the C_{g_2}-module V. Thence Part (i) implies Part (iii).

Conversely, if the C_{g_1}-module V is isomorphic to the C_{g_2}-module V, then there exists a group isomorphism $\varphi : C_{g_1} \to C_{g_2}$ and a k-vector space isomorphism $\psi : V \to V$ such that $(vg)\psi = (v\psi)(g^{\varphi})$, for every $v \in V$ and $g \in C_{g_1}$. This yields $g^{\varphi} = \psi^{-1} g \psi$, for every $g \in C_{g_1}$. Thence C_{g_1} is conjugate to C_{g_2} in $\mathrm{GL}_n(q)$ and Part (i) follows. $\square$

The set of abelian subgroups $\{C_{\mathrm{GL}_n(q)}(g) \mid V_g \text{ indecomposable}\}$ of $\mathrm{GL}_n(q)$ plays a very important role in this paper. It is worth to point out that, by Corollary 4.3, the conjugacy classes in this family of subgroups are in one-to-one correspondence with the ordered pairs of positive integers (d, m) with $n = dm$. We denote by

$$\{A_{d,m}\}_{d,m} \tag{4.4}$$

a set of representatives for these conjugacy classes. In particular, for $m = 1$, the group $A_{d,1}$ is a cyclic group, and actually $A_{d,1}$ is a maximal non-split torus of order $q^d - 1$ in $\mathrm{GL}_d(q)$, usually called a Singer cycle.

Lemma 4.5. *Let $d, m \geq 1$ be such that $n = dm$. The group $A_{d,m}$ is a maximal abelian subgroup of $\mathrm{GL}_n(q)$ and*

$$|N_{\mathrm{GL}_n(q)}(A_{d,m})| = \begin{cases} d(1 - q^{-d})^2 q^{2dm-d} & \text{if } m > 1, \\ d(1 - q^{-d}) q^d & \text{if } m = 1. \end{cases}$$

Proof. By definition of $A_{d,m}$, there exists an element $g = su$ of $A_{d,m}$ such that $A_{d,m} = C_{\mathrm{GL}_n(q)}(g)$, where s is the semisimple part of g and u is the unipotent part of g. By Lemma 4.2, we may choose $A_{d,m}$ such that $A_{d,m} \subseteq \mathrm{GL}_m(q^d)$ and we may assume that s is a scalar matrix of $\mathrm{GL}_m(q^d)$ of order $q^d - 1$.

By Lemma 4.2, $A_{d,m}$ is abelian. Let A be an abelian subgroup of $\mathrm{GL}_n(q)$ containing $A_{d,m}$ and x be in A. Since A is abelian, x commutes with g and so $x \in A_{d,m}$. This yields that $A_{d,m}$ is a maximal abelian subgroup of $\mathrm{GL}_n(q)$.

Let N be the normaliser in $\mathrm{GL}_n(q)$ of $A_{d,m}$ and x be in N. Since $\langle s\rangle$ is a normal Hall subgroup of $A_{d,m}$, we get that x normalises $\langle s\rangle$. So x normalises the subgroup of scalar matrices of $\mathrm{GL}_m(q^d)$. Thence, x acts as a Galois automorphism on the field $k[s]$ of order q^d. This shows that $|N : N \cap \mathrm{GL}_m(q^d)| = d$. If $m = 1$, then $\mathrm{GL}_1(q^d) = A_{d,1}$ and $|N| = d(q^d - 1)$. If $m > 1$, then Lemma 4.1 yields that $N \cap \mathrm{GL}_m(q^d)$ has order $(1 - q^{-d})^2 q^{2dm-d}$. $\square$

5. The family $\mathcal{A}_n(q)$ and the upper bound for $\omega(\mathrm{GL}_n(q))$

Finally, we are ready to study the family $\mathcal{A}_n(q)$ of abelian subgroups of $\mathrm{GL}_n(q)$ (given in Definition 1.6) necessary in order to obtain an upper bound on the size of $\omega(\mathrm{GL}_n(q))$. For convenience, we state Definition 1.6 again.

Definition 1.6. Let $\mathcal{A}_n(q)$ be the set of abelian subgroups A of $\mathrm{GL}_n(q)$ such that the A-module V has a decomposition $V_1 \oplus \cdots \oplus V_r$ into indecomposable A-modules satisfying the following properties:

- (i)**:** $A = A_1 \times \cdots \times A_r$, where $A_i \subseteq \mathrm{GL}(V_i)$;
- (ii)**:** for $i = 1, \ldots, r$, we have $A_i = C_{\mathrm{GL}(V_i)}(a_i)$, for some element $a_i \in \mathrm{GL}(V_i)$ such that $(V_i)_{a_i}$ is an indecomposable $k[t]$-module.

We show in Proposition 5.9 that, for $q > 2$, the elements of $\mathcal{A}_n(q)$ are maximal abelian subgroup of $\mathrm{GL}_n(q)$. From the definition of $\mathcal{A}_n(q)$ we get at once Theorem 1.5 (a).

Proposition 5.1. $\mathrm{GL}_n(q) = \cup_{A \in \mathcal{A}_n(q)} A$.

Proof. Given x in $\mathrm{GL}_n(q)$, consider a decomposition of $V_x = V_1 \oplus \cdots \oplus V_r$ into indecomposable $k[t]$-modules. The action of x on V_i is given by some element $a_i \in \mathrm{GL}(V_i)$. By Lemma 4.2, $A_i = C_{\mathrm{GL}(V_i)}(a_i)$ is abelian. Now, $x \in A = A_1 \times \cdots \times A_r$ and $A \in \mathcal{A}_n(q)$. $\square$

The following definition is necessary in order to have a natural set of labels for the elements in $\mathcal{A}_n(q)$ (see Lemma 5.3).

Definition 5.2. We denote by Φ the set of functions from $\{(d,m) \mid d,m \geq 1\}$ to $\mathbb{N}$. Also, we write Φ_n for the subset of Φ containing the functions μ such that $n = \sum_{d,m} dm\mu(d,m)$.

For instance, Φ_1 contains only one element, namely the function μ defined by $\mu(1,1) = 1$ and $\mu(d,m) = 0$, for $m > 1$ or $d > 1$.

Lemma 5.3. *The conjugacy classes of subgroups in $\mathcal{A}_n(q)$ are in one-to-one correspondence with the elements of Φ_n.*

Proof. We define a bijection θ from Φ_n to the set of conjugacy classes of subgroups in $\mathcal{A}_n(q)$. Let μ be in Φ_n. For each d,m and i with $1 \leq i \leq \mu(d,m)$, let $W_{d,m,i}$ be a k-subspace of V of dimension dm such that $V = \oplus_{d,m,i} W_{d,m,i}$. Note that this is possible because $\dim_k(V) = n = \sum_{d,m} dm\mu(d,m)$. Consider $A_{d,m}^{(i)} \leq \mathrm{GL}(W_{d,m,i})$, with $A_{d,m}^{(i)} = A_{d,m}$ as in Equation 4.4, and set $A = \prod_{d,m,i} A_{d,m}^{(i)}$. By construction, $A \in \mathcal{A}_n(q)$. Define $\theta(\mu)$ to be the conjugacy class containing A. Now, let $V = \oplus_{k=1}^{s} M_k$ be another decomposition of V into a direct sum of non-zero indecomposable A-submodules. By the Krull-Schmidt theorem [7, Theorem 14.5], there exists a bijective function f between the set of indices $\{(d,m,i) \mid 1 \leq i \leq \mu(d,m)\}$ and $\{1,\ldots,s\}$ such that $W_{d,m,i} \cong M_{f(d,m,i)}$. Thus, Corollary 4.3 yields that μ is uniquely determined from the conjugacy class of A in $\mathrm{GL}_n(q)$, that is, θ is injective.

The map θ is surjective by the definition of $\mathcal{A}_n(q)$. □

Given $\mu \in \Phi_n$, we denote by

$$A_\mu \tag{5.4}$$

a representative of the conjugacy class in $\mathcal{A}_n(q)$ corresponding to μ in Φ_n. We note that if $\mu(d,m) = 0$ for $m > 1$, then A_μ is a torus in $\mathrm{GL}_n(q)$. In particular, every maximal torus of $\mathrm{GL}_n(q)$ is a member of $\mathcal{A}_n(q)$.

Before proving the main result of this paper, we need first a definition and then some preliminary lemmas.

Definition 5.5. Let μ be in Φ_n and $q = 2$. We say that A_μ has *cyclic unipotent summand* if $\mu(1,x) = 0$ for all but at most one value of x, and if $\mu(1,x) \neq 0$ for $x = m$, say, then $\mu(1,m) = 1$. In particular, by Definition 1.6 and Lemma 4.2, V has at most one indecomposable A_μ-invariant summand W such that the action of

A_μ on W is given by the centralizer of a regular unipotent matrix (which is a cyclic matrix).

Lemma 5.6. *Let μ be in Φ_n. The decomposition of V as direct sum of indecomposable A_μ-modules is unique up to permutation of the summands if and only if either $q \geq 3$, or $q = 2$ and A_μ has cyclic unipotent summand.*

Proof. Let

$$V = \bigoplus_{\substack{d,m,\\ 1\leq i\leq \mu(d,m)}} V_{d,m}^{(i)}$$

be an A_μ-invariant direct decomposition in indecomposable modules labelled so that $\dim V_{d,m}^{(i)} = dm$ (see Lemmas 5.3). By Definition 1.6 (i), we have $A_\mu = \prod_{d,m,i} A_{d,m}^{(i)}$, where $A_{d,m}^{(i)} \subseteq \mathrm{GL}(V_{d,m}^{(i)})$.

Assume $q \geq 3$, or $q = 2$ and A_μ has cyclic unipotent summand. We show that the decomposition of V as direct sum of indecomposable A_μ-modules is unique, up to permutation of the summands. Let W be an indecomposable A_μ-invariant summand of V. Now, the A_μ-module W is cyclic, that is, there exists $v \in W$ such that $W = \langle v\rangle_{A_\mu}$ (where $\langle v\rangle_{A_\mu} = \langle va \mid a \in A_\mu\rangle$). Write $v = \sum_{d,m,i} v_{d,m}^{(i)}$, with $v_{d,m}^{(i)} \in V_{d,m}^{(i)}$. We claim that

$$W = \bigoplus_{d,m,i} \langle v_{d,m}^{(i)}\rangle_{A_\mu}. \tag{5.7}$$

The A_μ-module W is generated by $va = \sum_{d,m,i} v_{d,m}^{(i)}a$ (for $a \in A_\mu$), where $v_{d,m}^{(i)}a \in \langle v_{d,m}^{(i)}\rangle_{A_\mu}$. Therefore, $W \subseteq \sum_{d,m,i}\langle v_{d,m}^{(i)}\rangle_{A_\mu}$. Conversely, as $\langle v_{d,m}^{(i)}\rangle_{A_\mu} \cap \langle v_{d',m'}^{(i')}\rangle_{A_\mu} \subseteq V_{d,m}^{(i)} \cap V_{d',m'}^{(i')} = 0$ for $(d,m,i) \neq (d',m',i')$, it suffices to prove that $v_{d,m}^{(i)} \in W$ for every d,m,i. By Definition 1.6 (ii) and Lemma 4.2, the group $A_{d,m}^{(i)}$ contains a scalar matrix $s_{d,m}^{(i)}$ of $\mathrm{GL}_m(q^d)$ corresponding to a generator of $\mathbb{F}_{q^d}$ if $d \geq 2$, and to a primitive element of $\mathbb{F}_q$ if $d = 1$. In particular, $s_{d,m}^{(i)} \neq 1$ if $(q,d) \neq (2,1)$.

Assume first that $(q,d) \neq (2,1)$. Since $s_{d,m}^{(i)}$ acts as the identity matrix on $V_{d',m'}^{(i')}$ (for $(d',m',i') \neq (d,m,i)$), we get $vs_{d,m}^{(i)} = \sum_{(d',m',i')\neq(d,m,i)} v_{d',m'}^{(i')} + v_{d,m}^{(i)}s_{d,m}^{(i)}$. Therefore, $v_{d,m}^{(i)}(s_{d,m}^{(i)} - 1) = vs_{d,m}^{(i)} - v \in W$. As $s_{d,m}^{(i)}$ acts as a non-identity scalar matrix on $V_{d,m}^{(i)}$, we obtain $v_{d,m}^{(i)} \in W$. This yields that if $(q,d) \neq (2,1)$, then $v_{d,m}^{(i)}$

lies in W for every m and i. By hypothesis on q and A_μ and by Definition 5.5, we obtain that all but possibly one summand of v lies in W. The exceptional case $(q,d)=(2,1)$ occurs only if $q=2$ and $v_{1,m}^{(1)}$ is the only summand of v that is not covered by the argument in this paragraph; since $v\in W$, we get also in this case that $v_{1,m}^{(1)}\in W$ and hence that every summand of v lies in W. Our claim is now proved.

Since W is indecomposable, from Equation 5.7 we have $W=\langle v_{d,m}^{(i)}\rangle_{A_\mu}\subseteq V_{d,m}^{(i)}$ for some d,m,i. Since W is an A_μ-invariant summand and $V_{d,m}^{(i)}$ is indecomposable, $W=V_{d,m}^{(i)}$. As W is an arbitrary indecomposable summand of V, we get that $\{V_{d,m}^{(i)}\}_{d,m,i}$ are the only indecomposable summands of V and the decomposition is unique.

Conversely, assume that $q=2$ and A_μ does not have a cyclic unipotent summand, that is, $\mu(1,m)\geq 2$ for some m, or $\mu(1,m_1)=\mu(1,m_2)=1$ with $m_1\neq m_2$. Let V_1 and V_2 be two distinct A_μ-invariant indecomposable direct summands of V isomorphic to $V_{1,m}$ (if $\mu(1,m)\geq 2$) or isomorphic to V_{1,m_1} and V_{1,m_2} (if $\mu(1,m_1)=\mu(1,m_2)=1$). By Lemma 4.2, Equation 4.4 and Definition 1.6, V_i is an A_i-module, where $A_i=C_{\mathrm{GL}(V_i)}(u_i)$ and u_i is a regular unipotent matrix of $\mathrm{GL}(V_i)$. Let $v_{1,1},\dots,v_{1,r_1}$ (respectively, $v_{2,1},\dots,v_{2,r_2}$) be a k-basis of V_1 (respectively, V_2) such that $v_{i,j}^{u_i}=v_{i,j}+v_{i,j-1}$ (for $1<j\leq r_i$) and $v_{i,1}^{u_i}=v_{i,1}$ for $i=1,2$. Define $V_2'=\langle v_{2,1},\dots,v_{2,r_2-1},v_{1,1}+v_{2,r_2}\rangle$. Clearly, $V_1\oplus V_2=V_1\oplus V_2'$. We claim that V_2' is an indecomposable A_μ-invariant summand of V. Since u_2 is a cyclic matrix, $\mathrm{End}_{k\langle u_2\rangle}(V_2)$ is a polynomial algebra in u_2. Therefore, in order to show that V_2' is an A_μ-invariant summand of V, it suffices to show that V_2' is $\langle u_2\rangle$-invariant, which is clear from the definition of V_2' and from the action of u_2 on V_2.

As $V_{2'}\subseteq V_1\oplus V_2$, $V_2'\neq V_1$ and $V_2'\neq V_2$, we obtain that the decomposition of V as direct sum of indecomposable A_μ-modules is not unique. $\square$

We give a definition which is needed in Proposition 5.9 and in Section 6.

Definition 5.8. Let μ be in Φ_n and $V=V_1\oplus\cdots\oplus V_r$ be an A_μ-invariant decomposition of V in indecomposable modules. We write $\mathrm{Stab}(V,\mu)$ for the subgroup of $\mathrm{GL}_n(q)$ preserving the direct decomposition $V_1\oplus\cdots\oplus V_r$ of V, that is, $\mathrm{Stab}(V,\mu)=\{g\in\mathrm{GL}_n(q)\mid V_i^g\in\{V_1,\dots,V_r\}\text{ for every }i\}$.

We start by computing the size of the normaliser of a subgroup A_μ and by proving that, if $q \geq 3$ or $q = 2$ and A_μ has cyclic unipotent summand, then A_μ is a maximal abelian subgroup of $\mathrm{GL}_n(q)$, for $\mu \in \Phi$.

Proposition 5.9. *Let μ be in Φ_n. Then $|N_{\mathrm{GL}_n(q)}(A_\mu) \cap Stab(V,\mu)|$ equals*

$$\left(\prod_{d\geq 1}(d(1-q^{-d})q^d)^{\mu(d,1)}\mu(d,1)!\right)\left(\prod_{d\geq 1, m\geq 2}(d(1-q^{-d})^2q^{2dm-d})^{\mu(d,m)}\mu(d,m)!\right).$$

If either $q \geq 3$, or $q = 2$ and A_μ has cyclic unipotent summand, then $N_{\mathrm{GL}_n(q)}(A_\mu) \subseteq Stab(V,\mu)$, and A_μ is a maximal abelian subgroup of $\mathrm{GL}_n(q)$.

Proof. Let μ be in Φ_n. Write $A_\mu = \prod_{d,m} A_{d,m}^{\mu(d,m)}$, where $A_{d,m}$ is as defined in Equation 4.4. By Definition 5.8, we have

$$|N_{\mathrm{GL}_n(q)}(A_\mu) \cap \mathrm{Stab}(V,\mu)| = \prod_{d,m} |N_{\mathrm{GL}_{dm}(q)}(A_{d,m})|^{\mu(d,m)}\mu(d,m)!.$$

Applying Lemma 4.5, the equality in the proposition follows.

Assume that either $q \geq 3$, or that $q = 2$ and A_μ has cyclic unipotent summand. By Lemma 5.6, every element of $\mathrm{GL}_n(q)$ normalising A_μ induces a permutation of the indecomposable A_μ-submodules of V. Also, Corollary 4.3 yields that indecomposable A_μ-submodules are isomorphic if and only if they correspond to the same d, m. Therefore, $N_{\mathrm{GL}_n(q)}(A_\mu) \subseteq \mathrm{Stab}(V,\mu)$. Furthermore, by Lemma 4.5, $A_{d,m}$ is a maximal abelian subgroup of $\mathrm{GL}_{dm}(q)$ and so A_μ is a maximal abelian subgroup of $\mathrm{GL}_n(q)$. □

Remark 5.10. The converse of the last assertion of Proposition 5.9 is also true. Indeed, if $q = 2$ and A_μ does not have cyclic unipotent summand then $N_{\mathrm{GL}_n(q)}(A_\mu)$ contains an element x that does not lie in $\mathrm{Stab}(V,\mu)$ and $\langle A_\mu, x\rangle$ is abelian. Namely, in the notation of the last part of the proof of Lemma 5.6, the element x can be defined to act as the identity on all summands of the decomposition $\oplus_i V_i$, except those denoted $V_1 \oplus V_2$. The action of x on $V_1 \oplus V_2$ is given by $v_{i,j}^x = v_{i,j}$ except that $v_{1,1}^x = v_{1,1} + v_{2,r_2}$.

Next, we prove Theorem 1.5 (c).

Theorem 5.11. *$\mathcal{N}_n(q) \subseteq \mathcal{A}_n(q)$ with equality if and only if $q > n$.*

Proof. First we show that $\mathcal{N}_n(q) \subseteq \mathcal{A}_n(q)$. Let C be an element of $\mathcal{N}_n(q)$. By Definition 1.3, $C = C_{\mathrm{GL}_n(q)}(g)$ for some cyclic matrix $g \in \mathrm{GL}_n(q)$. Consider a decomposition of $V_g = V_1 \oplus \cdots \oplus V_r$ into indecomposable $k[t]$-modules. The action of g on V_i is given by some element $a_i \in \mathrm{GL}(V_i)$. By Lemma 4.2, $A_i = C_{\mathrm{GL}(V_i)}(a_i)$ is abelian. Now, $g \in A = A_1 \times \cdots \times A_r$ and $A \in \mathcal{A}_n(q)$. Replacing C by a conjugate if necessary, we may assume $A = A_\mu$, for $\mu \in \Phi_n$. Moreover since g is cyclic it follows that, if $q = 2$, then A has cyclic unipotent summand. So, by Proposition 5.9, A is a maximal abelian subgroup. As $g \in A$, we have $A \subseteq C_{\mathrm{GL}_n(q)}(g) = C$. Since C is abelian, we have $A = C$ and $C \in \mathcal{A}_n(q)$.

Finally, in the rest of the proof we show that $\mathcal{N}_n(q) = \mathcal{A}_n(q)$ if and only if $q > n$.

Assume $q > n$. As $\mathcal{N}_n(q) \subseteq \mathcal{A}_n(q)$, by Lemma 5.3, it suffices to prove that for every $\mu \in \Phi_n$ there exists a cyclic matrix $g_\mu \in A_\mu$ such that $A_\mu = C_{\mathrm{GL}_n(q)}(g_\mu)$. For every $d, m \geq 1$ such that $dm \leq n$, let $f_{d,m,1}, \dots, f_{d,m,\mu(d,m)}$ be irreducible polynomials of degree d. Note that since $q > n$, we may choose $f_{d,m,i}$ so that the polynomials $(f_{d,m,i})_{d,m,i}$ are pairwise distinct. Let

$$V = \bigoplus_{\substack{d,\, m, \\ 1 \leq i \leq \mu(d,m)}} V_{d,m}^{(i)}$$

be an A_μ-invariant direct decomposition in indecomposable modules labelled so that $\dim V_{d,m}^{(i)} = dm$ (see Lemmas 5.3). By Definition 1.6 (i), we have $A_\mu = \prod_{d,m,i} A_{d,m}^{(i)}$, where $A_{d,m}^{(i)} \subseteq \mathrm{GL}(V_{d,m}^{(i)})$. Also, by Definition 1.6 (ii), $A_{d,m}^{(i)} = C_{\mathrm{GL}(V_{d,m}^{(i)})}(h_{d,m}^{(i)})$, for some element $h_{d,m}^{(i)} \in \mathrm{GL}(V_{d,m}^{(i)})$ such that $V_{d,m}^{(i)}$ is an indecomposable $\langle h_{d,m}^{(i)} \rangle$-module. By Lemma 4.2 and Definition 4.4, $h_{d,m}^{(i)}$ is a cyclic matrix with minimum polynomial $p_{d,m,i}^m$, for some irreducible polynomial $p_{d,m,i}$ of degree d. Let $g_{d,m}^{(i)} \in \mathrm{GL}(V_{d,m}^{(i)})$ be a cyclic matrix with minimum polynomial $f_{d,m,i}^m$. Thence $V_{d,m}^{(i)}$ is an indecomposable $\langle g_{d,m}^{(i)} \rangle$-module. Set

$$g_\mu = \bigoplus_{\substack{d,\, m, \\ 1 \leq i \leq \mu(d,m)}} g_{d,m}^{(i)}.$$

Since $f_{d,m,i}$ and $p_{d,m,i}$ have both degree d, by Corollary 4.3 the groups $C_{\mathrm{GL}(V_{d,m}^{(i)})}(g_{d,m}^{(i)})$ and $C_{\mathrm{GL}(V_{d,m}^{(i)})}(h_{d,m}^{(i)}) = A_{d,m}^{(i)}$ are conjugate. So, by Definition 5.4 and by construction, g_μ is conjugate to an element in A_μ. Hence, replacing g_μ by a conjugate if

necessary, $g_\mu \in A_\mu$. The characteristic polynomial of g_μ is $\prod_{d,m,i} f_{d,m,i}^m$. As the polynomials $f_{d,m,i}$ are distinct, the characteristic polynomial of g_μ is equal to its minimum polynomial. Thence g_μ is a cyclic matrix. In particular, if $q = 2$, then at most one of the $f_{d,m,i}$ is $t+1$, and hence at most one of the $p_{d,m,i}$ is $t+1$. So, A_μ has cyclic unipotent summand; hence by Proposition 5.9, A_μ is a maximal abelian subgroup. As $C_{\mathrm{GL}_n(q)}(g_\mu)$ is abelian and $A_\mu \subseteq C_{\mathrm{GL}_n(q)}(g_\mu)$, we get $A_\mu = C_{\mathrm{GL}_n(q)}(g_\mu)$.

Assume $q \le n$. We need to prove that $\mathcal{N}_n(q) \subset \mathcal{A}_n(q)$. Let $\mu_0 \in \Phi_n$ be the map defined by

$$\mu_0(d,m) = \begin{cases} 0 & \text{if } d \ge 2 \text{ or } m \ge 2, \\ n & \text{if } d = 1 \text{ and } m = 1. \end{cases} \tag{5.12}$$

By Definition 5.4, A_{μ_0} is the group of diagonal matrices, that is, the split torus of size $(q-1)^n$. Since there are only $q-1$ distinct eigenvalues available, any $g \in A_{\mu_0}$ has an eigenvalue with multiplicity ≥ 2. Therefore, g is not a cyclic matrix and A_{μ_0} contains no cyclic matrices. Thus $A_{\mu_0} \in \mathcal{A}_n(q) \setminus \mathcal{N}_n(q)$. □

This allows us to complete the proof of Theorem 1.5.

Corollary 5.13. *$\omega(\mathrm{GL}_n(q)) \le |\mathcal{A}_n(q)|$ with equality if and only if $q > n$.*

Proof. The inequality $\omega(\mathrm{GL}_n(q)) \le |\mathcal{A}_n(q)|$ follows from Lemma 3.1 and Proposition 5.1. If $q > n$, then by Theorem 5.11 we have $\mathcal{A}_n(q) = \mathcal{N}_n(q)$. So, the inequality $\omega(\mathrm{GL}_n(q)) \ge |\mathcal{A}_n(q)|$ follows from Theorem 1.4. Now assume $q \le n$. Let μ_0 be the function in Φ_n defined in Equation 5.12 and $\mathcal{A}$ be the collection of subgroups A of $\mathcal{A}_n(q)$ not conjugate to A_{μ_0}. By Definition 5.4, A_{μ_0} is the group of diagonal matrices. Since there are only $q-1$ distinct eigenvalues available, every $g \in A_{\mu_0}$ has an eigenvalue with multiplicity ≥ 2. Therefore, every g is contained in some A, with $A \in \mathcal{A}$. Thus, from Proposition 5.1, we have $\mathrm{GL}_n(q) = \cup_{A\in\mathcal{A}} A$ and Lemma 3.1 yields $\omega(\mathrm{GL}_n(q)) \le |\mathcal{A}| < |\mathcal{A}_n(q)|$. □

Although Theorem 1.4 and Corollary 5.13 show that $N_n(q)$ and $\omega(\mathrm{GL}_n(q))$ are bounded above by $|\mathcal{A}_n(q)|$, the value and order of magnitude of $|\mathcal{A}_n(q)|$ is not easy to establish from the definition of $\mathcal{A}_n(q)$. Therefore, in the next section, we determine (for $q > 2$) a closed simple formula for the generating function $F(t)$ of $\{|\mathcal{A}_n(q)|/|\mathrm{GL}_n(q)|\}_{n\ge 1}$ (see Theorem 6.15). Also, in Section 7, by proving that

$F(t)$ is analytic on a certain disk in the complex plane, we determine the asymptotic behaviour of $|\mathcal{A}_n(q)|$, for $n \to \infty$.

6. A generating function

We start by defining two generating functions.

Definition 6.1. Let $F(t) = \sum_{n=1}^{\infty} a_n t^n$ be the generating function for the proportion $a_n = |\mathcal{A}_n(q)|/|\mathrm{GL}_n(q)|$ and $\overline{F}(t) = \sum_{n=1}^{\infty} b_n t^n$ be the generating function for

$$b_n = \sum_{\mu \in \Phi_n} |N_{\mathrm{GL}_n(q)}(A_\mu) \cap \mathrm{Stab}(V, \mu)|^{-1}$$

(see Definitions 5.4 and 5.8).

Remark 6.2. By Lemma 5.3, we get

$$a_n = \sum_{\mu \in \Phi_n} |N_{\mathrm{GL}_n(q)}(A_\mu)|^{-1}, \tag{6.3}$$

and so, by Definition 6.1, $a_n \le b_n$ for every n. Furthermore, by Proposition 5.9, $F(t) = \overline{F}(t)$ for $q \ge 3$. In particular, $F(t)$ and $\overline{F}(t)$ differ only when $q = 2$, in which case each coefficient b_n of $\overline{F}(t)$ is an upper bound for the coefficient a_n of $F(t)$. Since the generating function $\overline{F}(t)$ turns out to be easier to study, in the sequel we consider only $\overline{F}(t)$. This does not give rise to any restriction in the case of $q \ge 3$ and still provides an upper bound for $|\mathcal{A}_n(q)|$ when $q = 2$.

We note that Corollary 5.13 yields $a_n \ge \omega(\mathrm{GL}_n(q))/|\mathrm{GL}_n(q)|$ and, for $q > n$, $a_n = \omega(\mathrm{GL}_n(q))/|\mathrm{GL}_n(q)|$. So, by studying $\overline{F}(t)$, we shall determine a good description for $\omega(\mathrm{GL}_n(q))$. Namely, in Theorem 6.15 we prove a closed simple formula for the function $\overline{F}(t)$ and in Theorem 7.8 we give an exact formula for the limit $\lim_{n\to\infty} q^n b_n$.

Define the following two functions:

$$\begin{aligned} F_1(t) &= \prod_{d \ge 1} \exp\left(\frac{t^d}{d(1-q^{-d})q^d}\right), \\ F_2(t) &= \prod_{m \ge 2} \prod_{d \ge 1} \exp\left(\frac{t^{dm}}{d(1-q^{-d})^2 q^{2dm-d}}\right). \end{aligned} \tag{6.4}$$

Lemma 6.5. $\overline{F}(t) = F_1(t)F_2(t)$.

Proof. From the Taylor series for the exponential function $\exp(t)$ and from Definition 6.4, we have

$$
\begin{aligned}
(6.6)\qquad F_1(t) &= \prod_{d\geq 1}\left(\sum_{r=0}^{\infty}\frac{t^{dr}}{(d(1-q^{-d})q^d)^r r!}\right),\\
F_2(t) &= \prod_{m\geq 2}\left(\prod_{d\geq 1}\left(\sum_{r=0}^{\infty}\frac{t^{dmr}}{(d(1-q^{-d})^2q^{2dm-d})^r r!}\right)\right).
\end{aligned}
$$

By expanding the infinite products in Equation 6.6 for $F_1(t)F_2(t)$, in order to obtain a summand of degree n we have to choose (for each $d, m \geq 1$) a term of degree $dmr_{d,m}$ from the series

$$
\sum_{r=0}^{\infty}\frac{t^{dr}}{(d(1-q^{-d})q^d)^r r!}\ \text{(for } m=1) \quad \text{or} \quad \sum_{r=0}^{\infty}\frac{t^{dmr}}{(d(1-q^{-d})^2q^{2dm-d})^r r!}\ \text{(for } m>1),
$$

in such a way that $n = \sum_{d,m} dmr_{d,m}$. This yields that each summand of degree n obtained by expanding $F_1(t)F_2(t)$ is uniquely determined by an element $\mu \in \Phi_n$ (by setting $\mu(d,m) = r_{d,m}$). Hence, the coefficient of degree n in $F_1(t)F_2(t)$ is

$$
\sum_{\mu\in\Phi_n}\left(\prod_{d\geq 1}\frac{1}{(d(1-q^{-d})q^d)^{\mu(d,1)}\mu(d,1)!}\prod_{d\geq 1, m\geq 2}\frac{1}{(d(1-q^{-d})^2q^{2dm-d})^{\mu(d,m)}\mu(d,m)!}\right).
$$

Applying Proposition 5.9 and Equation 6.3, we see that the coefficient of t^n in $\overline{F}(t)$ equals the coefficient of t^n in $F_1(t)F_2(t)$. Thus $\overline{F}(t) = F_1(t)F_2(t)$. □

In the rest of this section we use the theory of symmetric functions to obtain a closed simple formula for the generating functions $F_1(t)$ and $F_2(t)$. We start by recalling some well-known results and definitions from [12]. Let $X = \{x_i\}_{i\geq 1}$ be an infinite set of variables and Λ be the *graded ring of symmetric functions* on X (see [12, Section I.2]). A *partition* is a sequence $\lambda = (\lambda_1, \lambda_2, \ldots)$ of non-negative integers in decreasing order and containing only finitely many non-zero terms. We write $|\lambda| = \sum_i \lambda_i$ and $X^\lambda = x_1^{\lambda_1}x_2^{\lambda_2}\cdots$. Let λ be a partition. The function

$$
m_\lambda(X) = \sum_{\alpha} X^\alpha
$$

summed over all distinct permutations α of λ is a symmetric function in Λ, and m_λ is called a *monomial symmetric function.* By definition, m_λ is a homogeneous

function of degree $|\lambda|$. For each $d \geq 0$ the dth *complete symmetric function* $h_d(X)$ is the sum of all monomial symmetric functions of degree d, so that

$$h_d(X) = \sum_{|\lambda|=d} m_\lambda(X).$$

The generating function for the complete symmetric functions is $H_X(t) = \sum_{d\geq 0} h_d(X)t^d$ (the label X in H_X is needed in order to record the set of variables X). It is proven in [12, (2.5), page 14] that

$$H_X(t) = \prod_{i\geq 1}(1 - x_i t)^{-1}. \tag{6.7}$$

For each $d \geq 1$ the dth *power sum symmetric function* is $p_d(X) = \sum_i x_i^d$. The generating function for the power sum symmetric functions is defined as $P_X(t) = \sum_{d\geq 1} p_d(X)t^{d-1}$. It is proven in [12, (2.10), page 16] that

$$P_X(t) = \frac{d}{dt}\log H_X(t). \tag{6.8}$$

From Equation 6.8, we see that $k + \sum_{d\geq 1} p_d(X)t^d/d = \log H_X(t)$, for some integer k. Since $H_X(0) = h_0(X) = 1$, we get that $\log H_X(0) = 0$ and so $k = 0$. Thence $H_X(t) = \exp(\sum_d p_d(X)t^d/d)$. This shows that

$$H_X(t) \quad = \quad \prod_{d\geq 1} \exp\left(\frac{p_d(X)t^d}{d}\right). \tag{6.9}$$

Write

$$\varphi_0(x) = 1 \qquad \text{and} \qquad \varphi_d(x) = (1-x)\cdots(1-x^d), \tag{6.10}$$

for $d \geq 1$.

In the following lemma we establish two simple formulae for $F_1(t)$.

Lemma 6.11. *(i):* $F_1(t) = \prod_{i\geq 0}(1 - q^{-(i+1)}t)^{-1}$;

(ii): $F_1(t) = \sum_{d=0}^{\infty} \frac{t^d}{q^d \varphi_d(q^{-1})}$.

Proof. Consider the set of variables $Q = \{q^{-(i-1)}\}_{i\geq 1}$, that is Q is obtained by specialising $x_i = q^{-(i-1)}$ (for $i \geq 1$). From [12, Example 4, page 19], we have that the dth power sum symmetric function $p_d(Q)$ on the set of variables Q satisfies

$p_d(Q) = (1-q^{-d})^{-1}$. So, Equation 6.9 yields

$$H_Q(q^{-1}t) = \prod_{d\geq 1} \exp\left(\frac{p_d(Q)t^d}{dq^d}\right) = \prod_{d\geq 1} \exp\left(\frac{t^d}{d(1-q^{-d})q^d}\right) = F_1(t).$$

Equation 6.7 gives $H_Q(q^{-1}t) = \prod_{i\geq 1}(1-q^{-(i-1)}(q^{-1}t))^{-1} = \prod_{i\geq 0}(1-q^{-(i+1)}t)^{-1}$ and (i) follows.

From [12, Example 4, page 19], we have that the dth complete symmetric function $h_d(Q)$ on the set of variables Q satisfies $h_d(Q) = 1/\varphi_d(q^{-1})$. Thus, we obtain $H_Q(t) = \sum_{d=0}^{\infty} t^d/\varphi_d(q^{-1})$ and $H_Q(q^{-1}t) = \sum_{d=0}^{\infty} t^d/q^d\varphi_d(q^{-1})$, which we showed above is $F_1(t)$, and (ii) is proved. □

The argument for obtaining a simple formula for $F_2(t)$ is very similar to Lemma 6.11, but a little trickier. We start with a definition. For each $m \geq 2$, define

$$F_2^{(m)}(t) = \prod_{d\geq 1} \exp\left(\frac{t^{dm}}{d(1-q^{-d})^2 q^{2dm-d}}\right). \tag{6.12}$$

Lemma 6.13. (i)**:** $F_2^{(m)}(t) = \prod_{i,j\geq 0}(1-q^{-(i+j+2m-1)}t^m)^{-1}$;

(ii)**:** $F_2(t) = \prod_{m\geq 2}\prod_{i,j\geq 0}(1-q^{-(i+j+2m-1)}t^m)^{-1}$.

Proof. Consider two infinite sets of variables $X = \{x_i\}_{i\geq 1}$ and $Y = \{y_i\}_{i\geq 1}$. From X and Y consider the infinite set of variables $Z = \{x_iy_j\}_{i,j\geq 1}$. By definition of the dth power sum symmetric function, we have

$$\begin{aligned} p_d(Z) &= \sum_{i,j\geq 1}(x_iy_j)^d = \sum_{i\geq 1} x_i^d\left(\sum_{j\geq 1} y_j^d\right) \\ &= \left(\sum_{i\geq 1} x_i^d\right)\left(\sum_{j\geq 1} y_j^d\right) = p_d(X)p_d(Y). \end{aligned} \tag{6.14}$$

Consider the set of variables $Q = \{q^{-(i-1)}\}_{i\geq 1}$ obtained by specialising $x_i = q^{-(i-1)}$ (or $y_i = q^{-(i-1)}$), for $i \geq 1$. Also, consider the set of variables $Q' = \{q^{-(i+j-2)}\}_{i,j\geq 1}$ obtained by specialising $x_iy_j = q^{-(i-1)}q^{-(j-1)}$. Under this assignment, we obtain from [12, Example 4, page 19] and Equation 6.14 that $p_d(Q') = p_d(Q)^2 = (1-q^{-d})^{-2}$.

Equation 6.9 yields

$$\begin{aligned} H_{Q'}(q(q^{-2}t)^m) &= \prod_{d\geq 1} \exp\left(\frac{p_d(Q')(q(q^{-2}t)^m)^d}{d}\right) = \prod_{d\geq 1} \exp\left(\frac{p_d(Q')t^{dm}}{dq^{2dm-d}}\right) \\ &= \prod_{d\geq 1} \exp\left(\frac{t^{dm}}{d(1-q^{-d})^2 q^{2dm-d}}\right) = F_2^{(m)}(t) \end{aligned}$$

using Equation 6.12. Finally, Equation 6.7 gives

$$H_{Q'}(q(q^{-2}t)^m) = \prod_{i,j\geq 1} (1-q^{-(i+j-2)}(q(q^{-2}t)^m))^{-1} = \prod_{i,j\geq 1} (1-q^{-(i+j+2m-3)}t^m)^{-1}$$

and (i) follows. Part (ii) follows from the definitions of F_2 and $F_2^{(m)}$ in Equations 6.4 and 6.12. $\square$

The following theorem gives a closed simple formula for $\overline{F}(t)$.

Theorem 6.15.

$$\overline{F}(t) = \left(\prod_{i=0}^{\infty}(1-q^{-(i+1)}t)^{-1}\right)\left(\prod_{m\geq 2, i,j\geq 0}(1-q^{-(i+j+2m-1)}t^m)^{-1}\right).$$

Proof. As $\overline{F}(t) = F_1(t)F_2(t)$, the theorem follows from Lemmas 6.11, 6.13. $\square$

By using the formula in Theorem 6.15 one can easily obtain the first few values of b_n, where $\overline{F}(t) = \sum_{n\geq 0} b_n t^n$. For instance, Table 1 in Section 1 was obtained by expanding the terms in t of degree ≤ 6 in the infinite products of $\overline{F}(t)$.

Using Lemma 6.11 (ii), we show that $\{q^n b_n\}_{n\geq 0}$ is an increasing sequence.

Theorem 6.16. *For each $n \geq 0$, $q^n b_n < q^{n+1} b_{n+1}$, where the b_n are as in Definition 6.1. Moreover, if $q > 2$ then the sequence $\{q^n|\mathcal{A}_n(q)|/|\mathrm{GL}_n(q)|\}_{n\geq 0}$ is increasing.*

Proof. Write $F_2(t) = \sum_{d\geq 0} c_d t^d$. It is clear from Equation 6.6 that $c_d \geq 0$. By Lemma 6.11, we have $F_1(t) = \sum_{d\geq 0} \frac{t^d}{q^d \varphi_d(q^{-1})}$ with φ_d as in Equation 6.10. Thus it follows from Lemma 6.5 that $b_n = \sum_{d=0}^{n} \frac{c_{n-d}}{q^d \varphi_d(q^{-1})}$. Now $\varphi_{d+1}(q^{-1}) = \varphi_d(q^{-1})(1 - q^{-(d+1)}) < \varphi_d(q^{-1})$ and $c_d \geq 0$, and hence

$$
\begin{aligned}
q^n b_n &= q^n \sum_{d=0}^{n} \frac{1}{q^d \varphi_d(q^{-1})} c_{n-d} = \sum_{d=0}^{n} \frac{1}{\varphi_d(q^{-1})} (q^{n-d} c_{n-d}) \\
&< \sum_{d=0}^{n} \frac{1}{\varphi_{d+1}(q^{-1})} (q^{n-d} c_{n-d}) = q^{n+1} \sum_{d=0}^{n} \frac{1}{q^{d+1} \varphi_{d+1}(q^{-1})} c_{n-d} \\
&= q^{n+1} \sum_{d=1}^{n+1} \frac{1}{q^d \varphi_d(q^{-1})} c_{n+1-d} \leq q^{n+1} \sum_{d=0}^{n+1} \frac{1}{\varphi_d(q^{-1})} c_{n+1-d} = q^{n+1} b_{n+1}.
\end{aligned}
$$

If $q > 2$, then $b_n = |\mathcal{A}_n(q)|/|\mathrm{GL}_n(q)|$ by Remark 6.2 and the definition of a_n, and the last assertion follows. $\square$

7. Analytic properties of the generating function $\overline{F}(t)$

Before studying analytically the functions $\overline{F}(t), F_1(t), F_2(t)$ we have to collect some numerical information that will be used later.

Lemma 7.1. *Set $l(q) = \prod_{k=1}^{\infty} (1 - q^{-k})^{-k(k+1)/2-1}$. We have:*

- (a)**:** *$l(q) > 1 + 2q^{-1} + 7q^{-2} + 19q^{-3}$;*
- (b)**:** *$l(q) < (1-q^{-1}-q^{-2})^{-1} \exp(q^{-1}/(1-q^{-1})^3) \exp(q^{-2}(1+q^{-1})/2(1-q^{-2})^4)$;*
- (c)**:** *for $q > 2$, $l(q) < 1 + 2q^{-1} + 7q^{-2} + 114q^{-3}$;*
- (d)**:** *if $q = 2$, then $395.0005 > l(2) > 278.98$.*

Proof. Part (a) follows by expanding in powers of q the first three terms $(1-q^{-1})^{-2}$, $(1-q^{-2})^{-4}$ and $(1-q^{-3})^{-7}$(for $k = 1, 2, 3$) of the infinite product $l(q)$ and noticing that $(1 - q^{-k})^{-1} > 1$, for $k \geq 1$.

Next, we consider an upper bound for $l(q)$. First, we recall that by the Binomial Theorem, $(1 - x)^{-s} = \sum_{k=0}^{\infty} \binom{k+s-1}{s-1} x^k$. In particular,

$$
(7.2) \qquad \sum_{k=1}^{\infty} \binom{k+1}{2} x^k = x \sum_{k=1}^{\infty} \binom{k+1}{2} x^{k-1} = x \sum_{k'=0}^{\infty} \binom{k'+2}{2} x^{k'} = \frac{x}{(1-x)^3}.
$$

Set $L(q) = \prod_{k=1}^{\infty} (1 - q^{-k})^{-k(k+1)/2}$. We have

$$\begin{aligned}
\log(L(q)) &= -\sum_{k=1}^{\infty}\frac{k(k+1)}{2}\log(1-q^{-k}) = \sum_{k=1}^{\infty}\frac{k(k+1)}{2}\left(\sum_{m=1}^{\infty}\frac{q^{-km}}{m}\right) \\
&= \sum_{m=1}^{\infty}\frac{1}{m}\left(\sum_{k=1}^{\infty}\binom{k+1}{2}q^{-km}\right) = \sum_{m=1}^{\infty}\frac{q^{-m}}{m(1-q^{-m})^3} \qquad (\dagger) \\
&< \frac{q^{-1}}{(1-q^{-1})^3} + \frac{1}{2}\sum_{m=2}^{\infty}\frac{q^{-m}}{(1-q^{-m})^3} \\
&< \frac{q^{-1}}{(1-q^{-1})^3} + \frac{1}{2(1-q^{-2})^3}\sum_{m=2}^{\infty}q^{-m} \\
&= \frac{q^{-1}}{(1-q^{-1})^3} + \frac{q^{-2}}{2(1-q^{-2})^3(1-q^{-1})},
\end{aligned}$$

where in $(\dagger)$ we used Equation 7.2. From [15, Lemma 3.5], we have $\prod_{k=1}^{\infty}(1-q^{-k})^{-1} < (1-q^{-1}-q^{-2})^{-1}$. Therefore, Part (b) follows.

Now, assume $q > 2$ and set $T = \exp(q^{-1}/(1-q^{-1})^3)$. So,

$$\begin{aligned}
T &= \sum_{r=0}^{\infty}\frac{(q^{-1}/(1-q^{-1})^3)^r}{r!} < \sum_{r=0}^{3}\frac{(q^{-1}/(1-q^{-1})^3)^r}{r!} + \sum_{r=4}^{\infty}\left(\frac{q^{-1}/(1-q^{-1})^3}{2}\right)^r \\
&= \sum_{r=0}^{3}\frac{(q^{-1}/(1-q^{-1})^3)^r}{r!} + \frac{\left(\frac{q^{-1}/(1-q^{-1})^3}{2}\right)^4}{1-\frac{q^{-1}/(1-q^{-1})^3}{2}} < 1+q^{-1}+\frac{7}{2}q^{-2}+41q^{-3},
\end{aligned}$$

where the first inequality uses $r! \geq 2^r$ (for $r \geq 4$) and the last inequality is obtained by expanding in powers of q and using the fact that $q > 2$.

With similar computations we get $\exp(q^{-2}(1+q^{-1})/2(1-q^{-2})^4) < 1+q^{-2}/2+2q^{-3}$ and $(1-q^{-1}-q^{-2})^{-1} < 1+q^{-1}+2q^{-2}+7q^{-3}$. Now, from Part (b) we have

$$\begin{aligned}
l(q) &< \left(1+q^{-1}+2q^{-2}+7q^{-3}\right)\left(1+q^{-1}+\frac{7}{2}q^{-2}+41q^{-3}\right)\left(1+\frac{1}{2}q^{-2}+2q^{-3}\right) \\
&< 1+2q^{-1}+7q^{-2}+114q^{-3}
\end{aligned}$$

and Part (c) follows.

The lower bound in Part (d) is obtained by computing $\prod_{k=1}^{30}(1-q^{-k})^{-k(k+1)/2-1}$ with $q = 2$ and the upper bound is obtained by substituting $q = 2$ in Part (b). $\square$

In the following two propositions, we study some analytic properties of $\overline{F}(t), F_1(t), F_2(t)$.

Proposition 7.3. *$F_1(t)$ is analytic on a disk of radius q. Also, $F_1(t)$ has a simple pole at $t = q$ and $(1 - q^{-1}t)F_1(t)$ is analytic on a disk of radius q^2.*

Proof. From Definition 6.4, we obtain

$$F_1(t) = \prod_{d=1}^{\infty} \exp\left(\frac{(q^{-1}t)^d}{d(1-q^{-d})}\right) = \exp\left(\sum_{d=1}^{\infty} \frac{(q^{-1}t)^d}{d(1-q^{-d})}\right). \tag{7.4}$$

Next, we determine where the series in Equation 7.4 is absolutely convergent. We get

(7.5)

$$\sum_{d=1}^{\infty} \frac{|q^{-1}t|^d}{d(1-q^{-d})} \leq \sum_{d=1}^{\infty} \frac{|q^{-1}t|^d}{1-q^{-d}} \leq \frac{1}{1-q^{-1}} \sum_{d=1}^{\infty} |q^{-1}t| = \frac{|q^{-1}t|}{(1-q^{-1})(1-|q^{-1}t|)}.$$

Since $1/(1 - q^{-1}t)$ is analytic on a disk of radius q and has a simple pole in $t = q$, the equivalent result for $F_1(t)$ follows at once.

It remains to show that $(1 - q^{-1}t)F_1(t)$ is analytic on a disk of radius q^2. Since $\varphi_r(q^{-1}) = \varphi_{r-1}(q^{-1})(1 - q^{-r})$ (for $r \geq 1$), from Lemma 6.11 (ii) we get

$$\begin{aligned}
(1-q^{-1}t)F_1(t) &= (1-q^{-1}t)\sum_{r=0}^{\infty} \frac{t^r}{q^r\varphi_r(q^{-1})} = 1 + \sum_{r=1}^{\infty}\left(\frac{t^r}{q^r\varphi_r(q^{-1})} - \frac{t^r}{q^r\varphi_{r-1}(q^{-1})}\right) \\
&= 1 + \sum_{r=1}^{\infty} \frac{q^{-r}t^r}{q^r\varphi_r(q^{-1})} = \sum_{r=0}^{\infty} \frac{t^r}{q^{2r}\varphi_r(q^{-1})}.
\end{aligned}$$

As,

$$\sum_{r=0}^{\infty} \frac{|t|^r}{q^{2r}\varphi_r(q^{-1})} \leq \prod_{i=1}^{\infty}(1-q^{-i})^{-1} \sum_{r=0}^{\infty} |q^{-2}t|^r = \prod_{i=1}^{\infty}(1-q^{-i})^{-1} \frac{1}{1-|q^{-2}t|},$$

we get that $(1 - q^{-1}t)F_1(t)$ is analytic on a disk of radius q^2. □

Proposition 7.6. *$F_2(t)$ is analytic on a disk of radius $q^{3/2}$.*

Proof. We argue as in Proposition 7.3. We have

$$\begin{aligned}
F_2(t) &= \prod_{m=2}^{\infty}\prod_{d=1}^{\infty} \exp\left(\frac{t^{dm}}{d(1-q^{-d})^2 q^{2dm-d}}\right) = \exp\left(\sum_{m=2}^{\infty}\sum_{d=1}^{\infty} \frac{t^{dm}}{d(1-q^{-d})^2 q^{2dm-d}}\right) \\
&= \exp\left(\sum_{d=1}^{\infty} \frac{t^{2d}q^d}{d(1-q^{-d})^2 q^{4d}} \sum_{m=0}^{\infty} \frac{t^{dm}}{q^{2dm}}\right) = \exp\left(\sum_{d=1}^{\infty} \frac{(q^{-2}t)^{2d}q^d}{d(1-q^{-d})^2(1-(q^{-2}t)^d)}\right).
\end{aligned}$$

Set $z = q^{-2}t$. We obtain

$$\log(F_2(t)) = \sum_{d=1}^{\infty} \frac{z^{2d}q^d}{d(1-q^{-d})^2(1-z^d)}. \tag{7.7}$$

We prove that for $|z| < q^{-1/2}$ (i.e. $|t| < q^{3/2}$) the series in Equation 7.7 is absolutely convergent. Note that

$$\left|\frac{1}{1-z^d}\right| \le \frac{1}{1-q^{-d/2}} \le \frac{1}{1-q^{-1/2}} \qquad \text{and} \qquad \frac{1}{d(1-q^{-d})^2} \le \frac{1}{(1-q^{-1})^2}.$$

Thus the series in Equation 7.7 is absolutely convergent if

$$\sum_{d=1}^{\infty} |z^2q|^d = \frac{1}{1-|z^2q|}$$

is absolutely convergent. As $|z| < q^{-1/2}$, we get $|z^2q| < 1$, so $F_2(t)$ is analytic for $|t| < q^{3/2}$. $\square$

We finally determine the asymptotic behaviour of $\{b_n\}_{n\ge1}$ (and so also for $\{a_n\}_{n\ge1}$ when $q > 2$).

Theorem 7.8. *We have*

$$l(q) = \lim_{n\to\infty} q^n b_n = \prod_{k=1}^{\infty}(1-q^{-k})^{-k(k+1)/2-1}$$

and also $|q^n b_n - l(q)| = o(r^{-n/2})$*, for every* $0 < r < q$.

Proof. From Propositions 7.3, 7.6, we get that $\overline{F}(t)$ is an analytic function on a disk of radius q, the point $t = q$ is a simple pole for $\overline{F}(t)$ and $f(t) = (1-q^{-1}t)\overline{F}(t)$ is an analytic function on disk of radius $q^{3/2}$. In particular, by [10, Lemma 1.3.3], we get that $\lim_{n\to\infty} q^n b_n = f(q)$ and $|b_n - f(q)/q^n| = o(r^{-3n/2})$, for every $0 < r < q$. In particular, it remains to compute $f(q)$.

From Lemma 6.13 (*ii*), we get $F_2(t) = \prod_{m\ge2,i,j\ge0}(1-q^{-(i+j+2m-1)}t^m)^{-1}$. In particular, $F_2(q) = \prod_{m\ge2,i,j\ge0}(1-q^{-(i+j+m-1)})^{-1}$. Now, given $k \ge 1$, there exist $k(k+1)/2$ choices of (i,j,m) such that $k = i+j+m-1$, with $m \ge 2$ and $i,j \ge 0$. Therefore, $F_2(q) = \prod_{k=1}^{\infty}(1-q^{-k})^{-k(k+1)/2}$.

From Lemma 6.11, we get $(1-q^{-1}t)F_1(t) = \prod_{i=1}^{\infty}(1-q^{-(i+1)}t)^{-1}$. So, $f(q) = \prod_{i=1}^{\infty}(1-q^{-i})^{-1}\prod_{k=1}^{\infty}(1-q^{-k})^{-k(k+1)/2}$ and the theorem follows. $\square$

Summing up, Theorem 1.7 follows from Theorems 6.16 and 7.8. Therefore, all the results mentioned in the introduction are now proved.

Remark 7.9. Since $|\mathrm{GL}_n(q)| = q^{n^2}\varphi_n(q^{-1})$, Theorem 7.8 yields that $b_n|\mathrm{GL}_n(q)|$ is a polynomial $p(q)$ in q of degree q^{n^2-n}. So, write $p(q) = \sum_{i=0}^{n^2-n} \alpha_i q^{n^2-n-i}$ and pick r such that $0 < r < q$.

As $|q^n b_n - l(q)| = o(r^{-n/2})$, we obtain that $|p(q) - q^{n^2-n}\varphi_n(q^{-1})l(q)| = o(r^{n^2-n-n/2}) = o(r^{n^2-3n/2})$. Furthermore, since $\varphi_n(q^{-1})l(q) = \prod_{k=n+1}^{\infty}(1-q^{-k})^{-1}\prod_{k=1}^{\infty}(1-q^{-k})^{-k(k+1)/2}$, we see that

$$\left|\sum_{i=0}^{n^2-n} \alpha_i q^{n^2-n-i} - q^{n^2-n}\prod_{k=1}^{\infty}(1-q^{-k})^{-k(k+1)/2}\right| = o(r^{n^2-3n/2}).$$

It follows that the first $\lfloor n/2 \rfloor$ coefficients $\alpha_0, \ldots, \alpha_{\lfloor n/2\rfloor - 1}$ are obtained from the series expansion of $\prod_{k=1}^{\infty}(1-q^{-k})^{-k(k+1)/2}$. Such a sequence is described and studied in [18].

Remark 7.10. It was conjectured in [2] that, for $q > n$,

$$\omega(\mathrm{GL}_n(q)) \geq q^{n^2-n} + \frac{|\mathrm{GL}_n(q)|}{q(q-1)^n} + \frac{|\mathrm{GL}_n(q)|}{q^{(n^2-n)/2}(q-1)^2}.$$

The second summand on the right hand side of this inequality is asymptotic to $q^{n^2-n-1} + (n-1)q^{n^2-n-2} + O(q^{n^2-n-3})$. Therefore, Remark 7.9 and Table 1 yields that this conjecture is incorrect for $n \geq 6$.

8. Concluding comments

We conclude by noticing that we can exploit the theory presented in this paper further in order to obtain a refinement of Corollary 5.13 in the case that $q \leq n$. We give an example in the case $n = q$ and $q > 2$.

From the proof of Theorem 5.11 we have that if $n = q$, then all A_μ (for $\mu \in \Phi_n$) are centralisers of cyclic matrices except if $\sum_m \mu(1,m) > q-1$. Since $q = \sum_{d,m}\mu(d,m)dm$, this implies $\sum_m \mu(1,m) = q$ and so $\mu = \mu_0$ where

$$\mu_0(d,m) = \begin{cases} 0 & \text{if } d \geq 2 \text{ or } m \geq 2, \\ q & \text{if } d = 1 \text{ and } m = 1. \end{cases}$$

By Definition 5.4, A_{μ_0} is the group of diagonal matrices, that is, the split torus of size $(q-1)^q$. By Proposition 5.9 we have $|N_{\mathrm{GL}_q(q)}(A_{\mu_0})| = (q-1)^q q!$.

Since there are only $q-1$ distinct eigenvalues available, any $g \in \mathrm{GL}_q(q)$ giving a decomposition of V_g as $\oplus_{i=1}^q V_i$ into 1-dimensional spaces has an eigenvalue with multiplicity ≥ 2. Therefore, we see that g is centralised by some cyclic matrix $g_\mu \in A_\mu$, for $\mu \neq \mu_0$. In particular, following the proof of Corollary 5.13 we have that

$$\omega(\mathrm{GL}_q(q)) = |\mathcal{A}_q| - \frac{|\mathrm{GL}_q(q)|}{(q-1)^q q!}.$$

It is not clear to the authors of this paper whether there is a general theory for small q and large n with a tractable formula for $\omega(\mathrm{GL}_n(q))$.

References

1. A. Abdollahi, A. Akbari, H. R. Maimani, Non-commuting graph of a group, *J. Algebra* **298** (2006), 468–492.
2. A. Azad, C. E. Praeger, Maximal sets of pairwise noncommuting elements of finite three-dimensional general linear groups, *Bull. Austral. Math. Soc.* **80** (2009), 91–104.
3. E. A. Bertram, Some applications of graph theory to finite groups, *Discrete Math.* **44** (1983), 31–43.
4. R. Brown, Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements, *J. Combin. Theory Ser. A* **49** No. 2 (1988), 294-307.
5. R. W. Carter, *Finite groups of Lie type, Conjugacy Classes and Complex Characters*, Wiley, Chichester, 1993.
6. A. M. Y. Chin, On non-commuting sets in an extra special p-group, *J. Group Theory* **8** (2005), 189–194.
7. C. W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras, Wiley, Pure and Applied Mathematics Volume XI, (1962).
8. J. D. Dixon, Maximal abelian subgroups of the symmetric groups, *Can. J. Math.* **23** (1971), 426–438.
9. J. Fulman, Cycle indices for the finite classical groups, *J. Group Theory* **2** (1999), 251–289.
10. J. Fulman, P. N. Neuman, C. E. Praeger, A Generating Function Approach to the Enumeration of Matrices in Classical Groups over Finite Fields, *Mem. Amer. Math. Soc.* **176**, (2005).
11. J. E. Humphreys, Conjugacy classes in semisimple algebraic groups, *Mathematical Surveys and Monographs* **43**, 1995.
12. I. G. Macdonald, Symmetric functions and Hall polynomials, Claredon Press, Oxford, (1979).
13. V. Faber, R. Laver and R. Mckenzie, Covering of groups by abelian subgroups, *Can. J. Math.* **30**, (1978), 933–945.
14. B. H. Neumann, A problem of Paul Erdős on groups, *J. Aust. Math. Soc. Ser. A* **21** (1976), 467–472.

15. P. M. Neumann , C. E. Praeger, Cyclic matrices over finite fields, *J. London Math. Soc.* **52** (1995), 263–284.
16. P. M. Neumann, C. E. Praeger, Cyclic matrices and the MEATAXE, *Ohio State Univ. Math. Res. Inst. Publ.* **8**, de Gruyter, Berlin, 2001, 291–300.
17. L. Pyber, The number of pairwise non-commuting elements and the index of the centre in a finite group, *J. London Math. Soc.* (2) **35** (1987), 287–295.
18. N. J. A. Sloane, Ed. (2008), The On-Line Encyclopedia of Integer Sequences, published electronically at `www.research.att.com/ njas/sequences/Sequence A000294`.
19. H. J. Tomkinson, Groups covered by finitely many cosets or subgroups, *Comm. in Algebra* **15** (1987), 845–859.
20. E. P. Vdovin, The number of subgroups with trivial unipotent radicals in finite groups of Lie type, *J. Group Theory* **7** (2004), 99–112.
21. G. E. Wall, Counting cyclic and separable matrices over a finite field, *Bulletin Australian Math. Soc.* **60** (1999), 253–284.

Azizollah Azad, Department of Mathematics,
Arak University, Arak, 38156-879, Iran.
E-mail address: `a-azad@araku.ac.ir`

Mohammad A. Iranmanesh, Department of Mathematics,
Yazd University, Yazd, 89195-741 , Iran
E-mail address: `iranmanesh@yazduni.ac.ir`

Cheryl E. Praeger, School of Mathematics and Statistics,
The University of Western Australia, Crawley, WA 6009, Australia
E-mail address: `praeger@maths.uwa.edu.au`

Pablo Spiga, School of Mathematics and Statistics,
The University of Western Australia, Crawley, WA 6009, Australia
E-mail address: `spiga@maths.uwa.edu.au`